REMARKS

Applicant respectfully requests reconsideration of this application, as amended, and consideration of the following remarks.

Amendments

Amendments to the Claims

Applicant has amended claims 1, 2, 6, 10, 24, 44, 55, 59, 62, 65, 78 and 81 to clarify that Applicant's invention operates to protect content in multiple formats. Applicant has further amended claim 2 to clarify that Applicant's invention limits use of content once the content is distributed to a client computer through a network. Claim 6 has been amended to correct a typographical error that caused the grammatical form of the claim to be improper.

Rejections

Rejections under 35 U.S.C. § 101

Claim 1 was rejected under 35 U.S.C. § 101 as lacking utility. The Examiner asserts that the invention claimed in claim 1 is inoperative because the claim contains no functionality. The Examiner also states that he cannot determined if claim 1 is a method or a process or a system or an article of manufacture as required by § 101.

Applicant respectfully traverses the rejection because claim 1 identifies a specific utility for the invention [MPEP 2107.01]. The functions of a browser are well-known to those of skill in the art. The limiting phrase "ephemeral-output-only" further defines the functions of the browser as would be apparent to one of skill in the art based on the ordinary meaning of the words of the phrase. The specific utility of the claimed invention

is described throughout Applicant's specification, e.g. page 7, lines 15-17 ("Ephemeral output, including view-only output, is visual or audio output that cannot be electronically reproduced or otherwise communicated by a computer system."). Furthermore, claim 1 as amended, claims additional functions for the ephemeral-output-only browser.

With regard to the asserted indefinite form of claim 1, Applicant considers claim 1 to be an apparatus claim.

Accordingly, Applicant respectfully requests the withdrawal of the rejection of claim 1 under 35 U.S.C. § 101.

Rejections under 35 U.S.C. § 102(e)

Claims 1-19 and 24-83 were rejected under 35 U.S.C. § 102(e) as being anticipated by Dykes, et al., U.S. Patent No. 5,872,915. Applicant respectfully traverses the rejection because Dykes does not disclose each and every element of the invention as claimed in claims 1-19 and 24-83.

Dykes discloses an authentication system that reduces the number of times a user has to send his/her authentication information to a networked server to access application programs running on the server. The user inputs data into a standard Web browser, such as Netscape or Internet Explorer, that causes the user's computer to send a request for access to a remote application program to a web server application. The web server application receives the access request and in response, requests the user input identifying information, e.g. a user ID, password and a key, which the web server application uses to authenticate the user. The key specifies the particular remote application program the user wishes to access. The web server application uses the user ID and password to authenticate the user, and passes the user ID and key to an application gateway if the user

is authenticated. The application gateway searches a user library for a matching user ID and key. If the application gateway finds a match, it logs the onto the application program using the information in the user library, and translates the user input into commands for the application program. The application program responds by sending data to the application gateway, which translates data into output that can be handled by the browser and then, in turn,. passes the data back to the browser for display to the user. Because the user library can contain multiple keys for a user, the user only has to be authenticated once by the web server application to access multiple remote application programs.

Dykes is teaches only a technique of authenticating a user for access to multiple application programs and does not disclose placing restrictions on the use of data from an application program once it is transferred to the user's (client) computer as claimed by Applicant. However, the Examiner is asserting that Dykes teaches a client program that limits the user's use of the content in the Abstract at lines 3-13, and in Figure 4, elements 220 and 330. The Abstract at lines 3-13 states:

> The system and method allows a user of the web browser to access the software application after performing appropriate security checks. The user inputs data via the web browser, which is communicated to the web server application. The web server application then authenticates the web browser, and passes appropriate input data to an application gateway, including data to uniquely identify the web browser. The application gateway then users authentication data received from the browser to determine whether the user of the browser is authorized to access the software application.

Applicant can find no disclosure in the Abstract related to a client program that limits the user's control over the use, in particular reproduction, of the data as asserted by

the Examiner. The Abstract describes a combination of server applications that authenticate the user before allowing the user to access a remote application program. It does not disclose limitations on the user of the data by a client program. With regard to elements 220 and 330 in Figure 4, the specification discloses both as server computers, while disclosing the applications they run, the web server application 222 and the application gateway 332 respectfully, as server applications, not client programs. Additionally, it is the server applications that control the user's access to the data, not a client program. Thus, the sections of Dykes relied on by the Examiner discloses only server applications that limit *access* to data on a remote server computer, not a client program that limits *use* of the data once it has been delivered to the client computer by the server computers.

The only client program disclosed by Dykes is the web browser. The browser is described as communicating with the web server application to send and receive data to/from the remote application program, which is the standard function of a browser. Dykes specifically states that any standard web browser is suitable for use with his invention. Based on this disclosure in Dykes, the Examiner asserts that standard browsers, such as Netscape and Internet Explorer, limit the user's control over the content displayed in the browser. Applicant strongly traverses the Examiner's characterization of standard browsers in general, and his interpretation of the functions of a browser as disclosed by Dykes.

First, the Examiner's characterization of standard browsers contradicts what is well-known to those skilled in the art. When a user browses a web site using, for example, Internet Explorer, picture, text, and other content is temporarily cached on the user's computer. If the user sees content that he/she wishes to permanently store on their

computer, the user can choose "File-Save As" from the menu bar, or right-click and choose "Save target as" or "Save picture as" to save the content to a mass storage device on the user's computer. Similar functions exist in all standard browsers and no standard browser restricts the user's control over the content once it is cached on the client computer.

Second, the functions of the browser described by Dykes does not include limiting the user's use of the content. The browser merely acts as a conduit for data and Dykes does not require that the browser perform any special functions: "Web browser 212 would include any web browser which is capable of transmitting and receiving data over the WWW." [Dykes: col. 4, lines 50-51]. Not only does the browser in Dykes not limit the user's use of the content, it does not even control the user's right to access the content; that function is performed by the server applications in Dykes.

Applicant now presents individual rebuttal arguments to the § 102 rejections of the claims as grouped by the Examiner.

Claim 1

Claim 1 claims an ephemeral-output-only browser. In his rejection of claim 1, the Examiner equates Applicant's ephemeral-output-only browser with the standard browser disclosed in Dykes. The Examiner is respectfully reminded that he must find each and every limitation of a claim in a reference to have a proper § 102 rejection of the claim over the reference. As stated above, standard browsers are not ephemeral-output-only browsers because they assert no control over the use of the content cached on the user's computer. Therefore, Dykes' cannot teach Applicant's express claim limitation of

"ephemeral-output-only" and Dykes does not anticipate Applicant's invention as claimed in claim 1.

Claims 2, 6-8, 10-19, 24-36, 40, 44-68 and 71-83

Amended independent claim 2, and claims 6-8 that depend from claim 2, recite a limitation that use of the content is limited once the content is distributed to the client computer. Dykes contains no disclosure regarding limiting use of the data once it has been sent to the user's computer and therefore Dykes cannot anticipate Applicant's invention as claimed in claims 2 and 6-8.

Independent claims 10, 59, 65, 78 and 81, from which claims 11-19, 60-61, 66-68, 71, 79-80 and 82-83 depend, all recite a limitation that reproduction of the content is either limited or prevented. Because Dykes does not disclose limiting or preventing reproduction of the data obtained from the application programs, Dykes cannot anticipate Applicant's invention as claimed in claims 10-19, 59-61, 65-68, 71, and 78-83.

Independent claims 24, 44, 55 and 62, from which claims 25-36, 40, 45-58 and 63-64 depend, all recite a limitation that the user prevented from using disallowed user functions. The Examiner has not cited any disclosure in Dykes that teaches such a limitation, and indeed there is no such disclosure in Dykes, and therefore Dykes cannot anticipate Applicant's invention as claimed in claims 24-36, 40, 44-58 and 62-64.

Claims 72-77 claim a secure document package data structure. The Examiner has not cited any disclosure in Dykes that teaches such a data structure. The only data structure disclosed in Dykes is the user library containing user name, password, database server identifier, and database identifier to provide the needed information to the gateway server application so it can login a user to a particular remote application program

identified by the key. The user library data structure has no elements in common with Applicant's claimed document package data structure. Therefore Dykes cannot anticipate Applicant's invention as claimed in claims 72-77.

Claims 3-5, 9, 69 and 70

Claim 3 depends from claim 2 and recites a further limitation that the client program is an ephemeral-output-only browser. As discussed above with reference to Claim 1, Dykes does not disclose and ephemeral-output-only browser and therefore Dykes cannot anticipate Applicant's invention as claimed in claim 3.

Claim 5 recites the limitation that reproduction of the content is limited, while claims 69 and 70 that depend from independent claims 2 and 65 thus recite the limitation the reproduction of the content is prevented. Because Dykes does not disclose limiting or preventing reproduction of the data obtained from the application programs, Dykes cannot anticipate Applicant's invention as claimed in claims 5, 69 and 70.

Claim 9 depends from claim 2 and recites further limitations of specific types of techniques that limit the user's control over the content. Dykes discloses none of those techniques and therefore Dykes cannot anticipate Applicant's invention as claimed in claim 1.

Claim 4

Claim 4 recites the limitation that reproduction of the content is limited through an add-in security module to the browser. The Examiner asserts that Dykes teaches an add-in security module for a browser. Applicant respectfully traverses the Examiner assertion because Dykes does not teach modifying a standard browser in any fashion and further because Dykes does not disclose limiting reproduction of the data obtained from

the application programs. Therefore, Dykes cannot anticipate Applicant's invention as claimed in claim 4.

Claims 37-39 and 41

Claims 37-39 and 41 all recite the limitation that the user is the user prevented from using disallowed user functions. Because there is disclosure in Dykes that teaches such a limitation, Dykes cannot anticipate Applicant's invention as claimed in claims 37-39 and 41.

Claims 42

Claim 42 depends from claim 24 and thus recites the limitation that disallowed user functions are disabled. Because there is disclosure in Dykes that teaches such a limitation, Dykes cannot anticipate Applicant's invention as claimed in claim 42.

Claims 43

Claim 43 depends from claim 24 and thus recites the limitation that disallowed user functions are disabled. Because there is disclosure in Dykes that teaches such a limitation, Dykes cannot anticipate Applicant's invention as claimed in claim 43.

Accordingly, Applicant submits that the invention claimed in claims 1-19 and 24-83 is not anticipated by Dykes under 35 U.S.C. § 102(e) and respectfully requests the withdrawal of the rejection of the claims.

New Claims

New claims 84-94 are allowable over Dykes because all recite the limitation that the content in a browser window is hidden if the browser window is not the foreground window and that limitation is not taught by Dykes.

SUMMARY

In this response, claims 20-23 have been canceled without prejudice in response to a restriction requirement, claims 2 and 6 have been amended, and new claims 84-94 have been added. Therefore, claims 1-19 and 24-94 are currently pending. In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Applicant respectfully requests reconsideration of the application and allowance of the pending claims.

If the Examiner determines the prompt allowance of these claims could be facilitated by a telephone conference, the Examiner is invited to contact Sue Holloway at (408) 720-3476.

Deposit Account Authorization

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR
& ZAFMAN LLP

Dated: April 19, 2001

Sheryl S. Holloway
Attorney for Applicant
Registration No. 37,850

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(408) 720-3476

VERSION OF AMENDED CLAIMS WITH MARKINGS

1. [Once Amended] An ephemeral-output-only browser that protects multiple formats of content received by the ephemeral-output-only browser.

2. [Once Amended] A system for protecting content distributed through a network comprising:

a client computer operable for connecting to the network and for executing a client program that is capable of protecting content in multiple formats and that limits [user control over] use of the content once the content is distributed to the client computer through the network; and

a server computer operable for connecting to the network and for executing a security program for securing the content distributed through the network.

6. [Once Amended] The system of claim 2, wherein the security program distributes the content to the client computer only when the client computer is executing the client program[, in at least one form, is limited].

10. [Once Amended] A method of enabling a provider to protect content distributed on a network comprising:

acquiring a server security program;

executing the server security program on a server computer connected to the network; and

distributing the content only to a client computer executing a limited-user client program which is capable of protecting content in multiple formats and limits at least one form of reproduction of the content [in at least one form].

24. [Once Amended] A method for controlling access to information presented by a web browser comprising:

presenting content within a browser window of the web browser, wherein the web browser is capable of protecting content in multiple formats; and

disabling a disallowed user function when the content is within the browser window.

44. [Once Amended] A computer-readable medium having stored thereon computer executable instructions to cause a client digital processing system and a server digital processing system to perform a method comprising:

transmitting content from the server digital processing system to the client digital processing system over a network;

presenting the content within a browser window on the client digital processing system, wherein the browser window is capable of protecting content in multiple formats; and

disabling a disallowed user function when the content is within the browser window, wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

55. [Once Amended] A client digital processing system for controlling access to content presented by a web browser, the client digital processing system comprising:

a processor;

a network interface logically coupled to the processor to receive the content;

a browser logically coupled to the network interface to present the content within a browser window; and

a security module capable of protecting content in multiple formats and logically coupled to the browser to disable disallowed user functions when the content is in the browser window, wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

59. [Once Amended] A server digital processing system for controlling access to content distributed to a client digital processing system, the server digital processing system comprising:

a processor;

a network interface logically coupled to the processor to receive a request for the content from the client digital processing system;

a server module logically coupled to the network interface to distribute the content to the client digital processing system in response to the request; and

a security module logically coupled to the server module to determine if the request is from a client digital processing system executing a limited-use client program which is capable of protecting content in multiple formats and prevents at least one form of non-ephemeral reproduction.

62. [Once Amended] A computer-readable medium having stored thereon computer executable instructions to cause a client digital processing system to perform a method comprising:

receiving protected content from a server digital processing system;

presenting the protected content within a browser window that is capable of protecting content in multiple formats; and

disabling disallowed user functions when the protected content is in the browser window, wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

65. [Once Amended] A computer-readable medium having stored thereon computer executable instructions to cause a server digital processing system to perform a method comprising:

receiving a request for protected content from a client digital processing system;

determining if the request is from a client digital processing system executing a limited-use client program that is capable of protecting content in multiple formats; and

distributing the protected content to the client digital processing system in response to the request only if the client digital processing system is executing the limited-use client program, wherein the limited-use client program prevents at least one form of non-ephemeral reproduction of the protected contents.

78. [Once Amended] A system for controlling reproduction of content on a client computer comprising:

means for receiving content to be protected; and

means for displaying the protected content on the client computer while preventing at least one form of reproduction of the content, wherein the means for displaying is capable of protecting content in multiple formats.

81. [Once Amended] A system for controlling reproduction of content stored on a server computer comprising:

means for protecting content stored on the server;

means for receiving a request for the protected content; and

means for determining if the request is from a requestor that is capable of protecting content in multiple formats and limits reproduction of protected content.